Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:55:17 UTC

Tool: JHUHUGIT

Names	JHUHUGIT Seduploader JKEYSKW Sednit Downrage GAMEFISH carberplike SofacyCarberp Carberp Trojan.Sofacy
Category	Malware
Type	Reconnaissance, Banking trojan, Backdoor, Info stealer, Dropper, Downloader
Description	(ESET) We define Seduploader as a two-binary component, comprising a dropper and the payload usually contained in this dropper. While those two have sometimes been used independently of each other, they usually are deployed together and remain the most-used first-stage malware of the Sednit group since the beginning of 2015. The payload component of Seduploader has been compiled for Windows and OS X, but our analysisis based solely on the Windows version. Nevertheless, the OS X version is very similar, and has been described by BAE Systems in June 2015.
Information	<https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/> <https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf> <https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/> <https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html> <https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/> <http://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html> <https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html>

	<http://www.welivesecurity.com/2015/07/10/sednit-apt-group-meets-hacking-team/> <http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/> <https://www.welivesecurity.com/2017/05/09/sednit-adds-two-zero-day-exploits-using-trumps-attack-syria-decoy/> <https://blog.xpnsec.com/apt28-hospitality-malware-part-2/> <https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed>
MITRE ATT&CK	<https://attack.mitre.org/software/S0044/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.seduploader> <https://malpedia.caad.fkie.fraunhofer.de/details/win.downrage>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:JHUHUGIT>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool JHUHUGIT

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=07298c2b-b4cd-4c87-ba6b-dce8e942e1da